UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/500,983	10/27/2004	Philipe Bressy	740612-186	3153

41972 7590 09/28/2007

LAW OFFICES OF STUART J. FRIEDMAN
28930 RIDGE ROAD
MT. AIRY, MD 21771

EXAMINER	
ZEE, EDWARD	
ART UNIT	**PAPER NUMBER**
2135	

MAIL DATE	DELIVERY MODE
09/28/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/500,983	BRESSY ET AL.	
	Examiner	Art Unit	
	Edward Zee	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *27 October 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *38-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *38-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 October 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/2/05, 11/14/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the preliminary amendment filed on July 6th, 2004. Claims 1-37 have been cancelled, Claims 38-47 have been added and Claims 38-47 are currently pending and have been considered below.

Specification

2. The abstract of the disclosure is objected to because the abstract contains more than 150 words. Correction is required. See MPEP § 608.01(b).

Claim Objections

3. Claim 46 is objected to because of the following informalities: the Examiner notes the use of the acronym "RAM" throughout this claim, while this is a old and well known term, the Applicant is still required to first provide a description in plaintext.

4. Claims 38 and 40 are objected to because of the following informalities: the Examiner notes that the word "date", in line 13 and 19 respectively, appears to be used in error and should be replaced with "data". Appropriate correction is required.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 43 and 46 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

7. Claim 43 recites the limitation "the secret personalized key" in line 2. There is insufficient antecedent basis for this limitation in the claim.

8. The term "high performance" in claim 46 is a relative term which renders the claim indefinite. The term "high performance" is not defined by the claim, the specification does not appear to provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

9. The Examiner will interpret Claim 46 as follows: "wherein the external memory includes a RAM and the chip has a bi-directional encryption/decryption hardware interface, wherein already encrypted data is exchanged between the chip and the RAM".

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 38-47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Candelore et al. (6,061,449) in view of Lacko SR. et al. (2001/0018745).

Claim 38: Candelore et al. discloses a method of protecting a device against unintended use in a secure environment, the device being adapted to execute applications that involve conditional

access to at least one of valuable contents and services, and the device including an integrated circuit that has a central processing unit, an internal memory and input/output connections for external memory incorporated on a single chip, comprising the steps of:

a. encrypting sensitive application code and data*(ie. program information)* with a secret key stored in a secured memory area of the internal memory for uniquely linking said external memory and said chip, the encrypted code and data being then stored in said external memory*(ie. the external storage device may be encrypted by encryption/decryption circuit)* [column 18, lines 66-67];

b. a random number generator which provides random numbers to the encryption/decryption circuit to create a random encryption sequence [column 23, lines 3-6];

c. appending authentication information in the form of a keyed hash to the program information and then encrypting the authenticated program information [column 19, line 1 & lines 50-59];

d. a small internal ROM can be used to store boot-up or other program information which may be required [column 28, liens 47-51].

However, Candelore et al. does not explicitly disclose:

a. encrypting a random number and a hash value of the random number with said secret key, the encrypted random number and hash value being decrypted with the secret key at least on each reset of the device;

b. and allowing decryption of the encrypted sensitive code and data only if the decrypted hash value equals a hash value calculated from the decrypted random number.

Nonetheless, Lacko SR. et al. discloses a similar method and further discloses a system initialization process which includes verifying a signature stored in the external memory with a public key retrieved from the boot ROM before continuing with the decryption of encrypted data stored on the external memory*(ie. program reads the signature portion and reads public key and verifies signature portion...if verified signature portion indicates that secure application is supported, then program starts operations)* [figure 5 & page 4, paragraph 0032 & 0034 & 0036].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to further perform the initial boot up verification process when performing the authentication/verification process disclosed by Candelore et al. in order to detect any malicious changes to the external memory while the system is powered down.

Claim 40: Candelore et al. discloses a method of protecting a device against unintended use in a secure environment, the device being adapted to execute applications that involve secure transactions and/or conditional access to valuable contents and/or services, and the device including an integrated circuit that has a central processing unit, an internal memory and input/output connections for external memory incorporated on a single chip, comprising the steps of:

a. signing any application code down-loaded into the device with a private key of an asymmetric key pair and proper execution of the application is subject to a verification of the signature with a public key of said key pair*(ie. the hashing of the data is keyed such that knowledge of a private key is required to generate the correct hash)* [column 20, lines 11-12];

b. encrypting sensitive application code and data*(ie. program information)* with a secret key stored in a secured memory area of the internal memory for uniquely linking said external

memory and said chip, the encrypted code and data being then stored in said external memory*(ie. the external storage device may be encrypted by encryption/decryption circuit)* [column 18, lines 66-67];

c. a random number generator which provides random numbers to the encryption/decryption circuit to create a random encryption sequence [column 23, lines 3-6];

d. appending authentication information in the form of a keyed hash to the program information and then encrypting the authenticated program information [column 19, line 1 & lines 50-59];

e. a small internal ROM can be used to store boot-up or other program information which may be required [column 28, liens 47-51].

However, Candelore et al. does not explicitly disclose:

a. encrypting a random number and a hash value of the random number with said secret key, the encrypted random number and hash value being decrypted with the secret key at least on each reset of the device;

b. and allowing decryption of the encrypted sensitive code and data only if the decrypted hash value equals a hash value calculated from the decrypted random number.

Nonetheless, Lacko SR. et al. discloses a similar method and further discloses a system initialization process which includes verifying a signature stored in the external memory with a public key retrieved from the boot ROM before continuing with the decryption of encrypted data stored on the external memory*(ie. program reads the signature portion and reads public key and verifies signature portion...if verified signature portion indicates that secure application is supported, then program starts operations)* [figure 5 & page 4, paragraph 0032 & 0034 & 0036].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to further perform the initial boot up verification process when performing the authentication/verification process disclosed by Candelore et al. in order to detect any malicious changes to the external memory while the system is powered down.

Claim 39: Candelore et al. and Lacko SR. et al. disclose a method of claim 38, and Candelore et al. further discloses that the application code is downloaded into the device, encrypted with the secret key and stored in the external memory*(ie. encryption/decryption circuit also receives the secret decryption key from a decryption key memory)* [column 27, lines 1-6].

Claim 41: Candelore et al. and Lacko SR. et al. disclose a method of claim 38, and Candelore et al. further discloses a unit dependent key which is unique to each decoder*(ie. unit key)* [column 24, lines 53-58], but does not explicitly discloses that it can be loaded on the chip after manufacturing.

However, Lacko SR. et al. further discloses a unique decoder key which can be programmed after manufacturing*(ie. chip identity register is programmable)* [page 3, paragraph 0027].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to further modify the key disclosed by Candelore et al. with this feature in order to provide a more flexible and customizable system.

Claim 42: Candelore et al. and Lacko SR. et al. disclose a method of claim 41, and Candelore et al. further discloses that the content of the secure memory area is protected by calculating a hash value of the secure memory area content and writing the hash value into the secure memory area*(ie. a key is successively hashed)* [column 25, lines 29-39].

Claim 43: Candelore et al. and Lacko SR. et al. disclose a method of claim 41, and Candelore et al. further discloses that a personalization application*(ie. program information)* is signed with a Secure Architecture Designer's private key*(ie. may include keys used to encrypt/decrypt or verify/authenticate the rest of the program information, authentication may be performed using PKI)* and then encrypted with the secret personalization key, the personalization application is loaded into the device and decrypted with the secret personalization key, the signature of the personalization application is checked with the Secure Architecture Designer's public key, and the personalization application is executed to write sensitive personalization data into the secure memory area*(ie. encrypted and optionally authenticated program information is transferred from the external storage device to the secure circuit)* [column 2, lines 9-24 & column 31, lines 15-22].

Claim 44: Candelore et al. and Lacko SR. et al. disclose a method of claim 41, and Candelore et al. further discloses that a personalization application*(ie. program information)* is encrypted with a secret symmetric key stored in a secured memory area of the device, a hash value*(ie. keyed hash)* of the personalization application is signed with a Secure Architecture Designer's private key*(ie. may include keys used to encrypt/decrypt or verify/authenticate the rest of the program information, which is optionally encrypted, thus does not need to be encrypted by a secret key)*, the encrypted personalization application and the signed hash value are loaded into the device, the personalization application is decrypted with the secret symmetric key, the signature of the hash value is checked with the Secure Architecture Designer's public key stored in the read only memory of the device, and the personalization application is executed to write sensitive personalization data into the secure memory area*(ie. encrypted and optionally authenticated*

program information is transferred from the external storage device to the secure circuit) [column 2, lines 9-24 | column 19, lines 1-2 & 55-59 | column 31, lines 15-22].

Claim 45: Candelore et al. and Lacko SR. et al. disclose a method of claim 41, and Candelore et al. further discloses that a personalization application*(ie. program information)* and a hash value*(ie. keyed hash)* of the personalization application signed with a Secure Architecture Designer's private key*(ie. may include keys used to encrypt/decrypt or verify/authenticate the rest of the program information)* are encrypted with a secret symmetric key stored in a secured memory area of the device, the encrypted personalization application and signed hash value are loaded into the device, the personalization application and signed hash value are decrypted with the secret symmetric key, the signature of the hash value is checked with the Secure Architecture Designer's public key stored in the read only memory of the device, and the personalization application is executed to write sensitive personalization data into the secure memory area*(ie. encrypted and optionally authenticated program information is transferred from the external storage device to the secure circuit)* [column 2, lines 9-24 | column 19, lines 55-59 | column 31, lines 15-22].

Claim 46: Candelore et al. and Lacko SR. et al. disclose a method of claim 38, and Candelore et al. further discloses that the external memory includes a RAM and the chip has a bi-directional encryption/decryption hardware and already encrypted exchange of data between the chip and the RAM*(ie. external storage device may be RAM or a combination of RAM and EEPROM, etc...desirable for content to be copied to faster storage such as synchronous dynamic memory)* [column 15, lines 57-67].

Claim 47: Candelore et al. and Lacko SR. et al. disclose a method according to claim 38, and Candelore et al. further discloses that said chip is provided with a random number generator and a hash value is obtained from a random number generated by the random number generator, the random number with its hash value are encrypted with said secret key, and the encrypted random number with its hash value are stored in the external memory*(ie. external storage device also stores authentication information, check bits, etc.)* [column 15, lines 57-67].

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Edward Zee whose telephone number is (571) 270-1686. The examiner can normally be reached on Monday through Thursday 9:00AM-5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KIM VU
SUPERVISORY PATENT EXAM
TECHNOLOGY CENTER 21